2011-05-00

Protecting Sensitive Information: The Virtue of Self-Restraint

Boyd, Dallas

Monterey, California. Naval Postgraduate School

Homeland Security Affairs (May 2011), v.7

Protecting Sensitive Information: The Virtue of Self-Restraint

Dallas Boyd

ABSTRACT

An abundance of information that could be useful to terrorists is available in the open literature. This information, unclassified but nonetheless sensitive, includes risk assessments that identify infrastructure vulnerabilities, analyses that hypothesize creative attacks, and otherwise dangerous knowledge that is released under the rubric of scientific openness or the public's "right to know." Attempts to manage this information more responsibly have been resisted in part due to the misconception that such efforts would require formal, draconian restrictions on speech. However, greater discipline in the dissemination of sensitive information can be introduced without compromising the nation's values. In particularly sensitive areas, scientists, journalists, and members of the general public should embrace voluntary self-restraint as a civic duty. Further, both government entities and journalists should avoid calling attention to sensitive information in ways that compound rather than reduce the potential harm it represents.

INTRODUCTION

Less than a year after the Cold War ended, one of its best-kept secrets came to light when the hidden purpose of West Virginia's Greenbrier Hotel was revealed in the *Washington Post*.[1] Beneath the hotel was a massive bunker built to house the U.S. Congress after a nuclear war, part of the nation's "continuity of government" program. Though congressional leaders had urged the newspaper not to expose the secret, the *Post's* executive editor justified the publication as a "historically significant and interesting story that posed no grave danger to national security or human life."[2] Ted Gup, the journalist who uncovered the Greenbrier's macabre function, went further, arguing that the facility had been potentially destabilizing even when its existence was a secret. Evacuating Congress during a crisis might have telegraphed that the United States was bracing for nuclear war, precipitating a Soviet first-strike. Far from an act of irresponsible journalism, Gup cited the story as a case study in the value of an inquisitive press corps.[3]

Though lawmakers quickly acknowledged the Greenbrier's obsolescence, the revelation remains controversial.[4] Despite a plea for discretion, a small number of journalists had substituted their own judgment on national security for that of the U.S. defense establishment. The tension that the story illuminated – between the value gained by revealing sensitive information and the potential harm invited by doing so – has only grown more pronounced since terrorism emerged as the dominant security threat. This tension usually concerns information that, like the bunker location, has been formally designated as secret. Most recently, WikiLeaks' release of more than a half-million classified documents has revived debate over the legitimacy of leaking as a form of civil disobedience.[5] However, a more complex question concerns the advisability of making public, or drawing attention to, a variety of mostly *unclassified* information that is nonetheless useful to terrorists.[6] Examples of this information include media descriptions of target vulnerabilities, hypothetical attack scenarios, and sensitive counterterrorism measures. The central question explored in this article is whether the availability of this unclassified knowledge benefits our adversaries more than it advantages society.

The motives behind disclosures of sensitive information vary, but a common refrain is that they spur remedial action that would otherwise be avoided. Critics argue, however, that these revelations recklessly endanger the public. Whatever their effect, a soft consensus seems to have formed that airing this information does not subtract from national security to such an extent as to justify the extraordinary powers that would be required to suppress it. This attitude

represents a stark departure from previous wartime policy, when speech was frequently restricted on security grounds.[7] During World War II, censorship succeeded largely because communications technology had not yet made the practice impractical. Since then, the information revolution has greatly expanded the number of people with access to sensitive information as well as the means to disseminate it. Attempts to manage this information have been less than vigorous, and in many cases the government itself has made questionable revelations in the name of greater transparency.

The existence of sensitive information in the public domain is a security concern only insofar as there are adversaries poised to exploit it. Yet on this score there can be little doubt. Gathering information from open sources is an established intelligence methodology that both states and non-state actors utilize. For example, Chinese physicists relied heavily on Western scientific literature in their development of strategic weapons.[8] Modern-day terrorists appear to behave similarly. A captured al-Qaeda training manual released by the Justice Department after 9/11 advises that by using public sources "openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy." Among the sources it recommends are "newspapers, magazines, books, periodicals, official publications, and enemy broadcasts."[9] The diversity of malevolent actors who might exploit this information has also grown dramatically over the previous decades. In the age of terrorism, the incoherence of the nation's response to this phenomenon represents a significant failure.

This article examines three common forms of "sensitive information," defined for the purpose of this analysis as knowledge that might be useful to terrorists *and* would be considerably more difficult – if not impossible – for them to assemble independently. This information includes: media reports and risk assessments, both private and government-sponsored, that identify critical vulnerabilities to terrorism; open-source analyses that hypothesize creative terrorist attacks; and publications that reveal potentially dangerous knowledge under the rubric of scientific openness or, in the case of classified information, the public's "right to know." The purpose of the analysis is to challenge the assumption that these revelations are largely innocuous. A further aim is to dispute the notion that curtailing them requires measures that are incompatible with our national values. This misconception encourages the belief that any effort to discourage discussion of sensitive information compromises civil liberties.

An alternative to draconian restrictions on speech entails fostering a culture of voluntary restraint, in which citizens refrain from inappropriate revelations out of a sense of civic duty. Its enforcement would depend not on government coercion but on individuals and institutions supplying disapproval of irresponsible discussion. Admittedly, any effort to discourage discussion of unclassified knowledge, no matter how sensitive, faces an obvious hurdle: persuading the public to accept new categories of protected information just as the government struggles to keep secret the materials it has already classified. But the challenge of safeguarding the two types of information is different. One requires more diligent enforcement of existing security protocols. The other is a societal responsibility that presents no additional burden to the government beyond promoting its merits. While the debate over the discussion of unclassified information is not likely to resume until another attack occurs, policymakers should revisit the matter before that inevitable event. In its aftermath, impulsive calls to curtail American rights may obscure the more measured option that is available today.

ADVERTISING VULNERABILITIES

The emergence of terrorism has occasioned the reevaluation of what had been a steady increase in transparency across many sectors of society. The shift in attitude concerning knowledge of natural gas line locations is instructive. For decades errant digging had occasionally punctured pipes containing explosive gas, with lethal results. Industry and government responded by advertising their location as widely as possible. After 9/11, however, a series of reports highlighting the possibility of natural gas attacks led some to question the wisdom of this effort. A 2004

New York Times headline captures the dilemma: "Mapping Natural Gas Lines: Advise the Public, Tip Off the Terrorists." In response to these concerns, pipeline maps began to be removed from many gas company web sites.[10] Similar fears have arisen in other countries. In 2008, flood risk experts in Britain's Environment Agency incurred the wrath of security officials when they published maps depicting regions under severe threat in the event of dam failures.[11] As in the United States, however, such objections have been inconsistent, leaving unresolved the question of whether society is better served by openness or discretion.

Reactions to the identification of vulnerabilities can generally be divided into two schools of thought. The first contends that vulnerability assessments are often indistinguishable from terrorists' target research and should therefore be closely guarded. In keeping with this view, Dennis Pluchinsky, a former State Department intelligence analyst, facetiously accused the American media of "treason" for its post-9/11 security coverage, which he suggested had "clearly identified for terrorist groups the country's vulnerabilities."[12] The opposing view is that identifying security gaps has a mostly salutary effect. As Georgetown Law Professor Laura Donohue argues, "Citizens are entitled to know when their milk, their water, their bridges, their hospitals lack security precautions. If discussion of these issues is censored, the state and private industry come under less pressure to alter behavior…"[13] Of course, these outcomes are not mutually exclusive – publicizing vulnerabilities may simultaneously alert terrorists to promising targets and prompt policymakers to protect them. In these cases, the crucial question is whether the benefit of identifying a vulnerability outweighs the possibility that the likelihood of its being exploited will increase. Since 9/11, many commentators have taken this wager, as a brief review of the literature illustrates.

In 2005, *Slate* writer Andy Bowers published instructions on how to exploit a loophole in the No-Fly List using online check-in. This convenience allows travelers to print boarding passes at home and proceed directly to airport security, where they present some form of government identification. While the names on the pass and ID must match, the Transportation Security Administration (TSA) does not scan the barcode or compare the name against the No-Fly List. Only at the gate is the boarding pass scanned, but no matching identification is required. Bowers suggests that terrorists could travel with two boarding passes – one legitimate, purchased with a stolen credit card, and the other a counterfeit created using widely available software. At the first checkpoint, the passenger will pass through as long as the fake pass corresponds with the ID. The scan of the genuine pass at the gate will not register alarm because it contains an innocent name. Bowers justified this revelation with a familiar defense – if he could discern the loophole, "any terrorist worth his AK-47 realized it a long time ago."[14] In another piece, journalist Jeffrey Goldberg provided a recipe for fabricating a homemade knife in flight with steel epoxy glue: "It comes in two tubes, one with steel dust and then a hardener. You make the mold by folding a piece of cardboard in two, and then you mix the two tubes together…. It hardens in 15 minutes."[15] Goldberg also described passing through security wearing under his shirt a polyurethane bladder designed to sneak 80 ounces of alcohol into sporting events, presumably sufficient to hold enough liquid explosives to destroy an aircraft in flight.[16]

A frequent target of journalistic exposés is the security surrounding the nation's critical infrastructure, particularly facilities that manufacture or store dangerous materials. In one "60 Minutes" investigation in 2004, camera crews infiltrated several chemical plants to demonstrate their susceptibility to terrorism.[17] Though these investigations often contain sensationalist or self-congratulatory undertones, such reporting can still be done responsibly. In 2005, for example, ABC News investigated the security at nuclear research reactors on 25 university campuses using undercover graduate students to penetrate the sites.[18] The laxity of the security would later be featured in a televised special on vulnerable nuclear sites. However, six weeks before the broadcast, the investigative team disclosed its findings to university officials and government personnel, allowing time to heighten security at the facilities. In doing so, a program that

might have instantly increased a security threat was limited to a mere embarrassment for the universities.

Government as the Source of Sensitive Information

Despite the practice of "overclassification," in which the government makes secret an abundance of innocuous material, government reports are ironically the source of much sensitive information.[19] The Smyth Report, the unclassified history of the Manhattan Project, provides a useful lesson.[20] Released in August 1945, the report had several purposes: to educate the public about the atomic bomb, showcase openness in government, and signal what could and could not be said about the new weapon. A debate raged over whether the report revealed too much –physicist Leó Szilárd claimed it "clearly indicates the road along which any other nations will have to travel" – but officials ultimately judged that nothing vital was revealed.[21] However, historian Michael Gordin argues that the Smyth Report was in fact "crucial for the Soviet [bomb] project—perhaps the most important single source of American information...." Thirty thousand translations were distributed to Soviet research institutes. According to Gordin, had the report not existed, "the Soviets would have had to write a guidebook of their own. Smyth saved them the trouble...."[22] Dr. Khidhir Hamza, an Iraqi weapon scientist who defected in 1994, recalled using the same materials in Saddam Hussein's nuclear program. He later wrote, "I was sure that if U.S. officials knew how valuable its Manhattan Project reports would be to us years later, they would have kicked themselves."[23]

The practice of revealing sensitive information for the sake of openness in government continues today. The Government Accountability Office (GAO), for example, regularly scandalizes Congress and the media with revelations of slipshod security practices. A typical report in 2007 described the ease with which undercover agents passed through airport security with concealed bomb components.[24] Beyond confirming the practicality of this attack mode, the report provided clues on the simulated bomb design that an astute terrorist might have perceived. A later report catalogued deficiencies in the security surrounding the nation's biosafety level 4 laboratories, which house pathogens such as Ebola and smallpox.[25] Another provided details of the behavioral profiling techniques that TSA uses to screen for suspicious airline passengers.[26] These reports are made public despite evidence that terrorists are aware of them. Indeed, in 2010, an al Qaeda affiliate released an English-language document detailing its attempt to detonate explosives on two U.S.-bound cargo aircraft; the document referenced a GAO assessment of cargo inspection methods, demonstrating the network's awareness of this source of information.[27]

These revelations would be beneficial if they consistently prompted corrective action, but in many cases they do not, as an earlier series of reports illustrates. In 2003, GAO provided a virtual guide to collecting material for a radiological dispersal device (RDD), which could easily be obtained due to weaknesses in the Nuclear Regulatory Commission's (NRC) licensing process.[28] Four years later, an investigation revealed that these weaknesses had not been addressed. After establishing a sham business with only a post office box, investigators acquired a license to receive radioactive materials and then doctored it to permit unlimited acquisition of sources. The investigators then contracted with two U.S. suppliers to purchase moisture density gauges containing enough americium-241 and cesium-137 to construct an RDD.[29] While this investigation finally forced the NRC to suspend its licensing program, the government has identified other security gaps where the potential for timely remediation is severely limited.

Numerous reports have advertised shortcomings in the architecture to detect smuggled nuclear weapons, particularly the inability of radiation portal monitors at U.S. seaports to detect "shielded" nuclear material.[30] Others have documented the virtual absence of scanning for railcars and small watercraft entering the country.[31] This information greatly reduces terrorists' uncertainty about the obstacles they face in conducting an attack. Micah D. Lowenthal draws on scholarship concerning criminal

behavior to demonstrate how this knowledge hinders our ability to deter nuclear terrorism. Specifically, he cites a study on the effectiveness of the Lojack car retrieval system, an unobservable transmitter that allows police to track stolen vehicles. While visible theft-deterrent devices such as steering wheel locks simply shift thieves' energies to neighboring cars, Lojack produced broad reductions in overall theft.[32] The explanation is simple: criminals are aware that the device is used but are unable to identify which cars have it. Lowenthal argues that a similar phenomenon may occur with nuclear terrorism, in which "the existence of some radiation monitoring at seaports and land border crossings may deflect adversaries, causing them to focus on other gaps…that are identified as easier targets."[33] Disclosing information on the detection architecture therefore guarantees that it will have little effect on the overall risk. By contrast, deliberate ambiguity about U.S. defenses might deter terrorists from attempting a nuclear attack in the first place. At the least, such a policy would avoid steering them toward the least defended entry points.

The preceding anecdotes concern attack vectors that are, in all likelihood, already familiar to terrorists. While this information may make an attack easier to plan or more likely to succeed, a determined adversary may be able to perform the necessary research without assistance. An altogether different category of sensitive information consists of novel ideas for attacks that may not have occurred to the most imaginative adversaries. Managing discussion of these scenarios presents a special challenge, as the creativity of the 9/11 attacks ensured that exercises in innovative thinking would find a receptive audience in both the government and the popular culture.

POSITING CREATIVE SCENARIOS

After 9/11, conceiving novel means of wreaking havoc became something of a fiendish hobby for many analysts.[34] One group of authors, noting the proliferation of hypothetical scenarios in the public domain, suggested that their source must be a basement where "thousands of monkeys who have yet to type out exact copies of the works of Shakespeare are nonetheless producing dozens of new ideas for attacks on America…"[35] Many of these scenarios follow a familiar template. "At 3 a.m. on a moonless night," begins one fictitious plot in *IEEE Spectrum*, "a pair of armored vans race down an access road leading up to the sprawling Hovensa oil refinery…."[36] Another scenario by Thomas Homer-Dixon (which begins at 4 a.m. on a "sweltering" night rather than a "moonless" one) involves an assault on the electricity grid during a heat wave:

> In different parts of [California], half a dozen small groups of men and women gather. Each travels in a rented minivan to its prearranged destination – for some, a location outside one of the hundreds of electrical substations dotting the state; for others, a spot upwind from key, high-voltage transmission lines…. Those outside the substations put together simple mortars made from materials bought at local hardware stores, while those near the transmission lines use helium to inflate weather balloons with long, silvery tails. At a precisely coordinated moment, the homemade mortars are fired, sending showers of aluminum chaff over the substations. The balloons are released and drift into the transmission lines. Simultaneously, other groups are doing the same thing along the Eastern Seaboard and in the South and Southwest. A national electrical system already under immense strain is massively short-circuited, causing a cascade of power failures across the country. Traffic lights shut off. Water and sewage systems are disabled. Communications systems break down. The financial system and national economy come screeching to a halt.[37]

Innumerable scenarios of this ilk have been described in the public domain, ranging from infecting livestock with contagious diseases to setting serial forest fires.[38] Security expert Bruce Schneier holds a perennial "Movie-Plot Threat Contest," inviting participants to propose attack scenarios that are "horrific and completely ridiculous, but plausible." The plots are reliably dramatic: irradiating Wall Street with radiological bombs, crashing explosives-filled

airplanes into the Grand Coulee Dam, and so on.[39] The government evidently sees value in such exercises, in part because the 9/11 Commission identified the failure of "imagination" as first among the deficiencies that contributed to the tragedy.[40] Shortly after the attacks, then-National Security Advisor Condoleezza Rice famously asserted, "I don't think anybody could have predicted that these people…would try to use an airplane as a missile."[41] Rice's statement was soon discovered to be incorrect – more than a dozen references to hijacked planes-cum-guided missiles were identified after the attacks. One 1999 report speculated that al Qaeda's suicide bombers "could crash-land an aircraft packed with high explosives…into the Pentagon, the headquarters of the [CIA], or the White House."[42]

The government subsequently commissioned a series of exercises to capture some of the creativity that had so disastrously eluded its analysts. In one program, the Army-funded Institute for Creative Technology enlisted Hollywood screenwriters and directors to conjure up frightening attack scenarios.[43] Yet the products of these sessions remained off-limits to public scrutiny. As one official explained, "Our worst nightmare was that we would suggest scenarios to terrorists."[44] Marvin Cetron, a "futurist" who credits himself with having foreseen the 9/11 attacks, claims that the State Department removed his prediction from a 1994 government report for fear that it might "give terrorists a valuable idea they might not conceive on their own."[45]

Cetron has found a more receptive market for his powers of discernment after 9/11 – he has since published several lists of "unthinkable" terrorist plots ranging from destroying Tennessee Valley Authority dams to bombing a liquefied natural gas tanker near a major city.[46] While such scenarios are often farcical, they occasionally produce useful insights. In one analysis, James Acton et al. suggest several innovative means of disseminating radiological materal beyond the standard "dirty bomb," in which radioactive material is simply mixed with explosives.[47] Though the common assumption is that such a device would produce catastrophic effects, the authors argue that the death toll would be "very unlikely to reach three figures." By contrast, attacks involving ingestion, inhalation, and immersion of radiation, which they dub I^3 attacks, may claim an order of magnitude more victims and would be less technically challenging to carry out.[48] While their analysis stops short of providing instructions to terrorists, the authors have arguably provided several kernels of useful information.

Just as in the case of advertising vulnerabilities, government officials are often the source of worrisome scenarios. In 2009, for example, Charles R. Gallaway, then head of the Domestic Nuclear Detection Office, testified before Congress on the challenge of interdicting attempts to smuggle a nuclear device into the United States. Citing a government study, he noted that "the most difficult scenario to counter was the use of [general aviation] aircraft delivering a weapon from outside the borders of the U.S. directly to a target." Gallaway observed that such an attack "would enable an adversary to bypass…multiple detection and interdiction opportunities."[49] Because a system to defeat this scenario would obviously require great time and expense to implement, and may ultimately be unachievable, the decision to emphasize this attack mode is curious. At the very least, Gallaway may have given adversaries inspiration that they did not previously possess.

On the question of giving terrorists novel ideas, commentators usually argue that our adversaries are sufficiently clever to discern the nation's vulnerabilities. As Cetron avers, "I no longer worry about giving the bad guys ideas…. They will think of any attack we can…"[50] Yet a private admission by al Qaeda leader Ayman al-Zawahiri casts doubt on this assumption. In a captured 1999 memo to an associate, Zawahiri conceded that "Despite their extreme danger, we only became aware of [biological and chemical weapons] when the enemy drew our attention to them by repeatedly expressing concerns that they can be produced simply with easily available materials."[51]

The year after Zawahiri's memo was written, columnist Colbert I. King authored a detailed scenario to highlight the capital's vulnerability. King described two heavily armed terrorists seizing control of the

Washington Monument, blocking the staircases with explosives, and firing from the windows with a .50 caliber rifle.[52] In his view, "Gain control of the monument and you hold sway over a large area of the world's most powerful capital, at least for several days." So attractive is the scenario, he suggests, that the monument "easily makes a terrorist's list."[53] Some variation of this rationale is the default response of those who publicly speculate about terrorist scenarios and wish to avoid criticism for doing so. However, an argument can be made that his attack had not occurred to a single terrorist before King described it. Elliot Panek considers this question in assessing the effect of "Wisdom of Crowds wiki-logic" in the context of terrorism, or whether aggregating creative scenarios constitutes "doing the terrorists' work for them."[54] He notes that generating plausible scenarios requires considerable thoughtfulness, and while "[o]ne writer (e.g., Tom Clancy) could be pretty good at that, and a bunch of devoted terrorists could be just as good if not better…a larger group of well-educated, creative people…would certainly be better at it than either Clancy or the terrorist." Panek rejects the assumption that terrorists have already conceived of every brilliant scenario, arguing that "the most sophisticated think tank is probably no match for the collective wisdom of the [*New York Times*] readership…"[55]

However irresponsible these descriptions, authors who publish them usually insist that terrorists could, with the proper effort and imagination, conceive them without assistance. The same is true for the identification of domestic vulnerabilities. What distinguishes the final species of information considered in this article is its inaccessibility to all but the most rarefied circle of thinkers. If the first two categories concern insights that would be difficult for adversaries to gain themselves, the last consists of information that requires the complicity of a third party.

PUBLISHING POTENTIALLY HARMFUL INFORMATION

Sensitive information is often revealed in the service of a beneficial purpose even if its immediate impact appears harmful. One famous case fitting this description is the *New York Times'* revelation of the Bush administration's domestic wiretapping program. After first learning of the program, the *Times'* refrained from publishing the story for a year, in part due to the urging of administration officials.[56] In December 2005, just before publishing their sensational scoop, journalist Eric Lichtblau and the newspaper's editors were summoned to the White House, where these officials again attempted to dissuade them from going to print. Their case was compelling: disclosure of the program would instantly eliminate its effectiveness and place American lives in danger. As Lichtblau later recounted, "the message was unmistakable: If the *New York Times* went ahead and published this story, we would share the blame for the next terrorist attack."[57] This argument was ultimately unpersuasive, although the *Times'* account of the program did omit certain sensitive details.[58] While the revelation was highly controversial—President Bush described it as "a shameful act" – the story prompted a constructive national debate on wartime executive power.[59] Many civil libertarians applauded the skepticism of a press corps that since 9/11 had been supine in its coverage of the administration's counterterrorism policies.

In other cases, dissemination of sensitive information resembles plain vandalism. This motive is evident in the work of John Young, founder of the web site Cryptome.org.[60] Young's hobby is to make public the government's most closely held secrets, his motivation appearing to extend no further than his conviction that "There's nothing that should be secret. Period."[61] Among the information he has published are the locations of nuclear weapon storage facilities and the home addresses of senior government officials.[62] In 2009, Young embarrassed TSA by posting an inadequately redacted manual that included airport metal detectors settings and a list of countries whose passport-holders require special scrutiny.[63] The following month he posted a similar document on screening procedures for explosive residue in checked baggage.[64] While these revelations have an impish quality, an argument can be made that they impose greater discipline on the government

to protect sensitive information, if only to avoid embarrassment. The same cannot be said for the amateur satellite trackers who gleefully publish the orbital inclinations of classified U.S. satellites. This phenomenon led a commission on the National Reconnaissance Office (NRO), which operates the nation's spy satellites, to note that "public speculation on how NRO satellites are used has aided terrorists and other potential adversaries in developing techniques of denial and deception to thwart U.S. intelligence efforts."[65] Despite this admonition, the practice continues, most recently in 2010 when the orbit of the Pentagon's classified X-37B spacecraft was revealed less than a month after its launch.[66]

Though the damage that results from these revelations may be quite severe, those who make them often belong to professions whose ethic sometimes requires disdain for government secrecy. In other cases the disseminators are everyday citizens with a penchant for mischief. In recent years, neither group has been particularly amenable to pleas for discretion. The government has had greater success in managing the communication of another cohort—scientists who conduct "dual-use" research. However, several recent lapses in caution among this group demonstrate the continued risk that attends the dissemination of sensitive information.

Dual-Use Scientific Research

In the early 1980s, many U.S. officials grew concerned that the Soviet Union was compensating for its technological inadequacy by mining the U.S. scientific literature. A 1982 incident conveys the climate at the time. Days before a major engineering conference, the Department of Defense (DoD) blocked the delivery of more than 100 unclassified papers on the grounds that Soviet bloc representatives would be present at the conference.[67] In response to the broader concern, the National Academy of Sciences (NAS) convened the Panel on Scientific Communication and National Security to explore tighter controls on academic communication.[68] While federal law grants broad authority to classify scientific research and thereby restrict its publication, deference to scientific openness had made the government reluctant to exercise this power.[69] The panel's findings, known as the Corson Report, acknowledged that a Soviet intelligence-gathering effort was directed at the American scientific community and that a substantial transfer of U.S. technology had indeed occurred. However, the panel determined that American universities, and open scientific communication more generally, were the source of very little of this transfer. Moreover, it concluded that formal policies to restrict scientific communication "could be extremely damaging to overall [U.S.] scientific and economic advance as well as to military progress." Calling for a strategy of "security by accomplishment" rather than secrecy, the report argued that the "limited and uncertain benefits of such controls are, except in isolated areas, outweighed by the importance of scientific progress..."[70] Though the demise of the Soviet Union appeared to vindicate this conclusion, the emergence of transnational terrorism revived the unease that inspired the Corson panel. Rather than the loss of military technology, recent anxieties have centered on publications in the life sciences and their potential utility to bioterrorists.

The danger of publishing sensitive scientific material was powerfully illustrated by a group of Australian scientists conducting pest control research in the late 1990s.[71] In a now-infamous experiment, the scientists inserted the interleukin-4 gene into the mousepox virus with the aim of producing an "infectious contraceptive" for mice.[72] Rather than sterilizing the subjects, however, the modified mousepox killed them, including many mice that had been immunized against the unaltered virus. The implications were ominous – a similar modification could yield vaccine-resistant viruses that are lethal to humans, including smallpox. Both the scientists and the editors of the journal to which the work was submitted understood its potential for misuse.[73] Their controversial decision to publish was based on the conclusion that the crucial elements of the research had already appeared elsewhere and that so much dangerous information was already available that one additional article would be inconsequential.[74] Nonetheless, the mousepox episode would be the catalyst for

yet another NAS study on the dangers of scientific communication.[75] Yet even before its commencement, scrutiny of dual-use research had greatly increased in the wake of the 9/11 attacks.

The dilemma in publishing such information is a familiar one. While certain scientific findings could aid malevolent actors, failing to air them in the open literature might inhibit research that holds the key to the defense. After contemplating this quandary, the American Society for Microbiology released guidelines in 2002 for reviewing manuscripts submitted to the journals under its purview. Under this voluntary process, peer reviewers would alert editors if material "might be misused or might pose a threat to public health safety," and a determination would be made concerning modifications.[76] (While only a handful of manuscripts have since been flagged, editors have deleted sensitive details on several occasions.[77]) The following year, the editors and publishers of the nation's leading life-science journals met to discuss the publication of such information. During this meeting, a near-consensus emerged that "there is information that…presents enough risk of use by terrorists that it should not be published." The group recommended that in circumstances in which the potential danger of publication exceeds the potential benefit to the public, sensitive papers should be modified or not published at all. In these cases, alternative means of communication such as academic seminars should be used to minimize the risk of misuse.[78] The eventual NAS report also reflected a preference for self-regulation, noting that "imposing mandatory information controls on research in the life sciences…[would] be difficult and expensive with little likely gain in genuine security."[79] As an alternative to government oversight, the NAS panel endorsed the concept of "voluntary self-governance of the scientific community rather than formal regulation by government."[80]

The presumption underlying this system is that scientists will censor themselves responsibly, obviating the need for government oversight, and that there will be agreement on what should not be published. The mousepox case calls both of these assumptions into question. After a review of the case, the editor of the *Journal of Virology* expressed no misgivings about the decision to publish.[81] Likewise, the NAS panel deemed the publication "appropriate," stating that there was "little technical information that was not already abundantly available in the literature."[82] Moreover, the research "alerted the scientific community to such a possibility occurring either intentionally or spontaneously."[83] However, at least one of the researchers involved in the experiment later expressed misgivings about its merit. Dr. Ian Ramshaw noted that even before discovering a method to increase the lethality of pox viruses, his team had stumbled upon another "dual-use dilemma" – creating an agent of contagious sterility – that was scarcely less sinister. As a weapon against humans, Ramshaw considered this "as bad as making a virus that kills the individual" and concluded that the original research "should never have started in the first place."[84]

Another article published after the NAS report reinforces the limits of self-censorship. In 2005, the *Proceedings of the National Academy of Sciences* approved for publication the research of Stanford University scholars Lawrence Wein and Yifan Liu, who had analyzed a release of botulinum toxin in the milk distribution system.[85] Wein and Liu had determined that absent detection, an attack involving less than 1g of the toxin would poison 100,000 people.[86] Among this exposed group, Wein later elaborated, more than half would likely perish.[87] Just prior to publication, an official of the Department of Health and Human Services requested that the journal hold the piece, calling it "a road map for terrorists."[88] After a brief delay to review the request, the editors proceeded with publication, which NAS president Dr. Bruce Alberts defended by noting that all of the information that could be useful to terrorists was "immediately accessible…through a simple Google search."[89] This is a familiar, yet spurious, defense. Putting aside that simply conceiving the attack mode is an important element of every plot, the existence of information on the Internet is not evidence of its harmlessness. Disparate, mundane information can be aggregated in such a way that the ultimate product is highly sensitive.

Aggregating Sensitive Public Information

The "Nth Country" experiment, a little-known exercise during the Cold War, illustrates the potential dividend that open-source research can yield. In 1964, the U.S. government recruited three young physics postdocs with no knowledge of nuclear weapons and tasked them with designing a bomb with a "militarily significant yield" using only open-source literature. To the dismay of many officials, their ultimate design was deemed workable.[90] In a later instance, journalist Howard Morland used public information and expert interviews to approximate the design of a hydrogen bomb, which he described in a piece for *Progressive* magazine.[91] After receiving a copy of the article, the government attempted to suppress its publication, setting off a highly public legal battle.[92] Only after similar information appeared in a separate publication – its author inspired by the *Progressive* case to commit an act of civil disobedience – did the government cease its attempt to silence Morland.[93]

A more recent case involves the doctoral dissertation of Sean Gorman, a George Mason University graduate student. Gorman and his research partner used public information culled from the Internet to map the fiber-optic network that connects American industry. The result was a tool that a government official described as a "cookbook of how to exploit the vulnerabilities of our nation's infrastructure."[94] According to its description in the press, the tool allowed a user to "click on a bank in Manhattan and see who has communication lines running into it and where… [or] drill into a cable trench between Kansas and Colorado and determine how to create the most havoc with a hedge clipper." When the pair presented their research to a room full of chief information officers of U.S. financial firms, it was suggested that they not be allowed to leave with their briefing. At the urging of government officials, the university directed that only general summaries of their findings be published.[95] This outcome, in which private citizens acted voluntarily to mollify the government, provides some optimism that sensitive information can be protected without formal restrictions. Yet the *ad hoc* nature of these interventions, and the absence of a culture of discretion that would make them unnecessary, ensures that much dangerous knowledge will continue to be available.

IMPLICATIONS

Perhaps the greatest obstacle to sanitizing discussion of sensitive information is the unresolved question of its harmfulness. Since 9/11, vulnerabilities have been identified in countless targets without terrorists' exploiting them. Several high-impact, easily replicable attacks have occurred and have not been copied. Consider, for example, the Beltway Sniper attacks, in which two snipers killed 10 people from a converted sedan in October 2002. These shootings fairly traumatized the Washington, D.C., area and are often cited as an ideal template for future attacks.[96] Yet after eight years no similar attack has occurred. The few attacks that have been attempted, such as Najibullah Zazi's 2009 plot to bomb the New York City subway, have required no special choreography or insight into security gaps.[97] While this observation might explain the complacency surrounding sensitive information, a spectacular attack may quickly invalidate it, especially if such information turns out to have enabled its success. The danger of disseminating sensitive information should be evaluated *a priori* and not on the basis of recent experience.

If one accepts the premise that sensitive information may be useful to attentive adversaries, the central question is how to manage this information more appropriately. Previous wartime restrictions on speech are neither politically acceptable nor technologically feasible in the present day. Perhaps the most famous of these is the 1917 Espionage Act, which criminalized the transmission of "information relating to the national defense" to the country's enemies.[98] Latter-day incarnations of this law were proposed after 9/11, such as Dennis Pluchinsky's suggestion—risible even in those fearful days – that laws should be enacted "temporarily restricting the media from publishing any security information that can be used by our enemies."[99] Such proposals

have little chance of enactment, but variations are being pursued that are only slightly less troubling. The following discussion examines the efficacy of the government's usual approach to managing sensitive information. Additionally, several alternatives are put forward that are both less intrusive and potentially more effective than the bald restrictions on speech that are often proposed.

The Perils of Censorship

Even when the government has legitimate objections to the release of information, either classified or merely sensitive, efforts to suppress its publication occasionally backfire.[100] This occurred in 1979 when the government attempted to censor Howard Morland's hydrogen bomb article. Hugh E. DeWitt, a retired government physicist, noted then that the genesis of the controversy was the Department of Energy's (DOE) response to *Progressive's* editors, who had submitted Morland's manuscript for confirmation of its technical accuracy. According to DeWitt, "Had [DOE] responded with their usual curt 'no comment' the article would have appeared, attracted little attention, and been quickly forgotten."[101] The pursuit of an injunction implicitly confirmed the value of its content. A similar episode unfolded in late 2010 when the Pentagon purchased and destroyed 9,500 copies of *Operation Dark Heart*, the memoir of a former intelligence officer in Afghanistan.[102] DoD officials had determined that the book contained classified operational details. However, because dozens of advance copies had already been distributed, comparison of the censored second printing with the original work allowed for the identification of its sensitive revelations.[103] As a result of the publicity, the redacted version of the book soon topped Amazon's bestseller list.[104]

Still more vexing than protecting appropriately classified information, which the government has a clear justification to safeguard, is managing the potential harm of unclassified information in the public domain. As *Science* Editor-in-Chief Donald Kennedy notes, "[government officials] can't order the nonpublication of a paper just because they consider the findings 'sensitive.' No such category short of classification exists..."[105] Often the appropriate response is not to impose formal restrictions at all, which are likely to be ineffective, incompatible with the First Amendment, or both. Indeed, the government's inability to silence WikiLeaks illustrates its impotence in policing speech in the Internet age.[106] Public leaders should instead promote a culture of voluntary restraint, in which gratuitous revelations of sensitive information are collectively frowned upon. After 9/11, the government took tentative steps to encourage this approach, but they rarely extended beyond the advice issued by the National Infrastructure Protection Center, which asked Americans to "apply common sense in deciding what to publish on the Internet."[107] While many commentators would ignore any request to refrain from publishing sensitive information, even a small reduction in irresponsible discussion would be preferable to the current paradigm.

Self-restraint as a Civic Duty

Changes in societal mores are probably more responsible than any technological development for the increased traffic in sensitive information. Irresponsible disclosures frequently occur without any social penalty for those who make them. This represents a dramatic shift from earlier generations, when cooperation with the government on security matters was more uniform. In one well-known example, American physicists refrained from publishing results on nuclear fission experiments during World War II for fear of assisting the Nazi bomb program.[108] Even among provocateurs, there is precedent for self-restraint. Daniel Ellsberg's name is synonymous with exposing government secrets, having leaked the Pentagon Papers. Yet Ellsberg conscientiously withheld four volumes regarding sensitive negotiations out of concern that they would disrupt the peace process.[109] Such discretion can still be found, although it is uncommon enough to be conspicuous. In their analysis of radiological terrorism, for example, James Acton et al. stopped short of revealing a radiation immersion scenario that they claimed would "readily kill several hundreds and disrupt a large city." As for the specifics of the plot, they wrote, "We will not describe it."[110] In an

earlier episode, the government sought a voluntary embargo of the details of a 1984 incident in which religious cultists poisoned 751 people in Oregon with *Salmonella*. Fearing the attack would inspire copycats, officials asked the *Journal of the American Medical Association* to refrain from describing the method for twelve years; the editors agreed.[111]

As an alternative to formal restrictions on communication, professional societies and influential figures should promote voluntary self-censorship as a civic duty. As this practice is already accepted among many scientists, it may be transferrable to members of other professions. As part of this effort, formal channels should be established in which citizens can alert the government to vulnerabilities and other sensitive information without exposing it to a wide audience. Concurrent with this campaign should be the stigmatization of those who recklessly disseminate sensitive information. This censure would be aided by the fact that many such people are unattractive figures whose writings betray their intellectual vanity. The public should be quick to furnish the opprobrium that presently escapes these individuals.

The need to influence the behavior of scientists is particularly acute. The Corson panel, while expressing little enthusiasm for restrictions on scientific communication, noted the existence of a category of research that merited "limited restrictions short of classification" on a largely voluntary basis. This category represented a "gray area" lying between research that can be discussed openly and that which the government has good cause to classify.[112] While the need for voluntary self-censorship among scientists is already well recognized, there is still some resistance to the idea that scientific communication should ever be constrained. To wit, one of the researchers involved in the Australian mousepox experiment defended their publication on the grounds that "Anything scientifically interesting should be published."[113] An effort must be made to temper this attitude and make clear that the pursuit of scientific knowledge does not absolve researchers of their social responsibility.

An understandable objection to self-censorship arises when one considers that huge quantities of *classified* information are being maliciously leaked under the auspices of WikiLeaks. It might seem curious to criticize well-meaning professionals for discussing unclassified information that is far less damaging than the genuine secrets being revealed. Yet the nihilism of this small group is not the standard against which one's actions should be measured. Nor does it release conscientious citizens from their duty not to endanger the nation.

Self-censorship among Journalists

Outside of the laboratory, discretion in national security matters is nowhere more important than in the field of journalism. The World War II-era Office of Censorship owed much of its success to the voluntary cooperation of the press.[114] The relationship between the government and the media is more adversarial today, but vestiges of past cooperation remain. For example, in journalist Bob Woodward's account of the 2007 troop "surge" in Iraq, he pointedly refused to describe a secret technology used to target insurgent leaders, which he credited with much of the campaign's success.[115] In other cases, however, journalists' carelessness has caused considerable damage to the nation's security. The authorized biography of Timothy McVeigh provides a useful example. Based on interviews with McVeigh, two journalists described in detail the bomb he used in the Oklahoma City attack, including its triply redundant fusing mechanism.[116] Because information that appears in major newspapers or works from leading publishing houses bears a certain institutional imprimatur, terrorists may find it useful. Would-be bombers face the dilemma of not knowing which of the multitude of Internet bomb designs are feasible, and operational security may preclude their testing a device. Given that McVeigh's design had been dramatically demonstrated, detailed instructions on how to replicate it should not have been provided.[117]

Even more important than omitting certain sensitive details is to refrain from sensational reporting that magnifies rather than diminishes security threats. Calling

attention to alarming information, ostensibly to prompt its redress, may instead compound the danger, especially if a remedy is not practicable. Once such incident took place in 1975 when Britain's *Sunday Times* reported that the U.K. patent office had allowed the formerly secret formula for the VX nerve agent to be published.[118] British officials scrambled to remove the offending documents from public libraries.[119] However, far from eliminating a threat, the story drew attention to information that was already widely available, having been declassified in several countries years before.[120] One British patent agent noted that "without the indiscretion of the *Sunday Times* an amateur would have been unable to identify and locate the relevant document."[121] Worse, according to Geoffrey Forden, the *Times* story was the catalyst that initiated Iraq's nerve gas program.[122] Another example can be found in the reporting on the WikiLeaks releases. Several media outlets described a leaked State Department cable that listed sites around the world whose destruction would "critically impact" U.S. national security. Among these were African mines that produce cobalt and bauxite as well as locations where underwater communications cables reach land. One article defended these revelations on the specious grounds that "any would-be terrorist with Internet access and a bit of ingenuity might quickly have identified" the sites.[123] Yet as a result of this carelessness, a terrorist would require neither ingenuity nor the patience to scour thousands of leaked documents to identify the most sensitive information.

Journalists should be encouraged to resist the notoriety that attends such reporting by appeals to their sense of civic responsibility. However, it is not the purpose of this essay to suggest that self-censorship should always be the default response when sensitive information is obtained. The media's role in exposing government incompetence plays a crucial function in maintaining the nation's civic hygiene, and revealing secrets is occasionally necessary for this purpose. Yet for revelations that potentially threaten public safety, a set of criteria should be established that assist the media in choosing responsibly between silence and disclosure. Regarding security vulnerabilities, the crucial question is whether the potential exists for timely remediation. If it does not, little is gained by drawing attention to weaknesses in the nation's defenses. An additional determinant should be whether alternative mechanisms exist to alert the government to a deficiency. Here the government has a clear responsibility to ensure that public exposés are not the only means to correct a shortcoming in security.

CONCLUSION

Whatever the excesses of the U.S. response to 9/11, avoiding wholesale restrictions on the discussion of sensitive information represents a triumph of moderation. Yet in our reverence for free expression, communication has been tolerated that carries considerable security risks while delivering questionable benefits to society. Greater discipline can be imposed on the discussion of sensitive information without formal, coercive restrictions on speech. Indeed, this effort should be predicated on forestalling even greater erosions of liberties that may occur after another devastating attack.

Just as the evolution of social mores has been a factor in making irresponsible communication more acceptable, efforts to discourage these discussions should center on challenging their basic appropriateness. Civic and professional leaders possess considerable power to influence popular perception. This power should be harnessed to place the burden of policing irresponsible discussion squarely in the hands of the public. Its success will ultimately be achieved not by coercion but by persuasion – specifically, by convincing citizens that the government is not the sole arbiter of the sensitivity of information and that responsibility for protecting the nation extends to every citizen who possesses it.

About the Author

Dallas Boyd *is a national security analyst with Science Applications International Corporation (SAIC). Mr. Boyd received a BA degree in history from The Citadel and a Master in Public Policy*

degree from Harvard University's John F. Kennedy School of Government. Mr. Boyd performs research and analysis for U.S. government customers concerning terrorism, U.S. counterterrorism policy, nuclear deterrence, and adversary decision-making. His current work involves assessing emerging technology threats to U.S. national security. Mr. Boyd may be contacted at dallas.g.boyd@saic.com.

ACKNOWLEDGEMENT

The author thanks Nash'at Ahmad, James Beard, Matthew Kutilek, Stephen J. Lukasik, Al Mauroni, Joshua Pollack, and two anonymous reviewers for their constructive comments on earlier drafts of this article. These reviews significantly clarified his thinking and writing.

[1] Ted Gup, "The Ultimate Congressional Hideaway," *Washington Post Magazine*, May 31, 1992, http://www.washingtonpost.com/wp-srv/local/daily/july/25/brier1.htm.

[2] Kenneth J. Cooper, "Hill Leaders 'Regret Reports on Bomb Shelter Site," *Washington Post*, May 30, 1992.

[3] Susan Glaser, "Ted Gup's disclosure of the Greenbrier bunker still controversial 17 years later," *Plain Dealer*, March 13, 2009, http://blog.cleveland.com/pdextra/2009/03/ted_gups_disclosure_of_the_gre.html.

[4] House Majority Leader Richard Gephardt called the bunker a "relic of the Cold War which probably ought to be mothballed," a view shared by House Speaker Thomas S. Foley. See Kenneth J. Cooper, "Foley Urges Closing W.Va. Bomb Shelter," *Washington Post*, June 3, 1992.

[5] Greg Jaffe and Karen DeYoung, "Leaked files lay bare war in Afghanistan," *Washington Post*, July 26, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/07/25/AR2010072502092.html; Greg Miller and Peter Finn, "Secret Iraq war files offer grim new details," *Washington Post*, October 23, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/10/22/AR2010102201682.html; Glenn Kessler, "Leaked cables expose U.S. diplomacy," *Washington Post*, November 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/28/AR2010112802395_pf.html.

[6] The term "sensitive information" is used for the purpose of this article only and is not to be confused with the formal security designation "Sensitive but Unclassified" (SBU), which, until its replacement by the category Controlled Unclassified Information (CUI) in May 2008, included such categories of information as For Official Use Only (FOUO), Critical Infrastructure Information (CII), and many others. For further information on SBU, see Genevieve J. Knezo, "'Sensitive But Unclassified' Information and Other Controls: Policy and Options for Scientific and Technical Information," Congressional Research Service, December 29, 2006, http://www.fas.org/sgp/crs/secrecy/RL33303.pdf.

[7] See Michael S. Sweeney, *Secrets of Victory: The Office of Censorship and the American Press and Radio in World War II* (Chapel Hill: The University of North Carolina Press, 2001).

[8] Evan A. Feigenbaum, *China's Techno-Warriors: National Security and Strategic Competition from the Nuclear to the Information Age* (Stanford: Stanford University Press, 2003), 65; see also John Wilson Lewis and Xue Litai, "Strategic Weapons and Chinese Power: The Formative Years," *China Quarterly* 112 (December 1987): 546, http://www.jstor.org/stable/653778.

[9] *Al Qaeda Training Manual*, "Eleventh Lesson – Espionage: Information-Gathering Using Open Methods," Excerpts released by the U.S. Justice Department, December 6, 2001, http://www.fas.org/irp/world/para/manualpart1.html.

[10] Ian Urbina, "Mapping Natural Gas Lines: Advise the Public, Tip Off the Terrorists," *New York Times*, August 29, 2004, http://www.nytimes.com/2004/08/29/nyregion/29pipeline.html. In another example, the Government Printing Office issued a request in October 2001 that federal depository libraries destroy any copies of a U.S. Geological Survey CD-ROM entitled "Source Area Characteristics of Large Public Surface-Water Supplies in the Conterminous United States: An Information Resource for Source-Water Assessment, 1999." The request was made in response to fears that the CD-ROM could be useful to terrorists plotting chemical or biological attacks. See Laura Taddeo, "Information Access Post September 11: What Librarians Need to Know," *Library Philosophy and Practice* 9, no. 1 (Fall 2006), http://www.webpages.uidaho.edu/~mbolin/taddeo.htm. For an analysis of the security implications of open-source geospatial information, including the location and physical characteristics of critical infrastructure, see John C. Baker, et al., *Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information* (Santa Monica, CA: RAND Corporation, 2004), http://www.rand.org/pubs/monographs/MG142/.

[11] Michael McCarthy, "MI5: revealing areas at mercy of collapsing dams is a terror threat," *The Independent*, June 26, 2008, http://www.independent.co.uk/environment/climate-change/mi5-revealing-areas-at-mercy-of-collapsing-dams-is-a-terror-threat-854325.html

[12] Dennis Pluchinsky, "They Heard It All Here, And That's the Trouble," *Washington Post*, June 16, 2002.

[13] Laura K. Donohue, "Censoring Science Won't Make Us Any Safer," *Washington Post*, June 26, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/06/25/AR2005062500077.html

[14] Andy Bowers, "A Dangerous Loophole in Airport Security," *Slate*, February 7, 2005, http://www.slate.com/id/2113157.

[15] Jeffrey Goldberg, "The Things He Carried," *Atlantic Monthly*, November 2008, http://www.theatlantic.com/magazine/archive/2008/11/the-things-he-carried/7057/.

[16] Ibid.

[17] Rebecca Leung, "U.S. Plants: Open To Terrorists," CBS News 60 Minutes, June 13, 2004, http://www.cbsnews.com/stories/2003/11/13/60minutes/main583528.shtml.

[18] "Script: Radioactive Road Trip 10/05," ABC News, October 13, 2005, http://abcnews.go.com/WNT/story?id=1855424&page=1.

[19] For a succinct discussion of the problem of "overclassification," see Steven Aftergood, testimony before the Senate Judiciary Subcommittee on the Constitution, hearing on Restoring the Rule of Law, Washington, DC, September 16, 2008, http://www.fas.org/irp/congress/2008_hr/091608aftergood.pdf.

[20] The official title of the report, written by Princeton University Physics Department Chairman Henry DeWolf Smyth, was *Atomic Energy for Military Purposes: The Official Report on the Development of the Atomic Bomb under the Auspices of the United States Government, 1940-1945* (Princeton, NJ: Princeton University Press, 1945), http://nuclearweaponarchive.org/Smyth/index.html

[21] Michael Gordin, *Red Cloud at Dawn: Truman, Stalin and the End of the Atomic Monopoly* (New York: Farrar, Straus, and Giroux, 2009), 91-104.

[22] Ibid.

[23] Khidhir Hamza with Jeff Stein, *Saddam's Bombmaker: The Daring Escape of the Man Who Built Iraq's Secret Weapon* (New York: Simon & Schuster, 2000), 69.

[24] "Aviation Security: Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process," Government Accountability Office report GAO-08-48T, November 15, 2007, http://www.tsa.gov/assets/pdf/gao_report.pdf.

[25] "Biosafety Laboratories: Perimeter Security Assessment of the Nation's Five BSL-4 Laboratories," Government Accountability Office report GAO-08-1092, September 2008, http://www.gao.gov/new.items/d081092.pdf.

[26] "Aviation Security: Efforts to Validate TSA's Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges," Government Accountability Office report GAO-10-763, May 2010, http://www.gao.gov/new.items/d10763.pdf.

[27] Al-Qaeda in the Arabian Peninsula, "Inspire: Special Issue," November 2010, 19, http://www.investigativeproject.org/documents/testimony/375.pdf

[28] "Nuclear Security: Federal and State Action Needed to Improve Security of Sealed Radioactive Sources," General Accounting Office report GAO-03-804, August 2003, http://www.gao.gov/new.items/d03804.pdf.

[29] "Nuclear Security: Actions Taken by NRC to Strengthen Its Licensing Process for Sealed Radioactive Sources Are Not Effective," Government Accountability Office report GAO-07-1038T, July 12, 2007, http://www.gao.gov/new.items/d071038t.pdf.

[30] "Combating Nuclear Smuggling: DHS Improved Testing of Advanced Radiation Detection Portal Monitors, but Preliminary Results Show Limits of the New Technology," Government Accountability Office report, GAO-09-655, May 2009, http://www.gao.gov/new.items/d09655.pdf; and "Combating Nuclear Smuggling: Recent Testing Raises Issues About the Potential Effectiveness of Advanced Radiation Detection Portal Monitors," Government Accountability Office testimony, GAO-10-252T, November 17, 2009, http://www.gao.gov/new.items/d10252t.pdf. See also National Research Council, *Evaluating Testing, Costs, and Benefits of Advanced Spectroscopic Portals for Screening Cargo at Ports of Entry: Interim Report*, Committee on Advanced Spectroscopic Portals (Washington, DC: The National Academies Press, 2009), http://books.nap.edu/catalog.php?record_id=12699.

[31] "Combating Nuclear Smuggling: DHS Has Made Some Progress but Not Yet Completed a Strategic Plan for Its Global Nuclear Detection Efforts or Closed Identified Gaps," Government Accountability Office testimony, GAO-10-883T, June 30, 2010, http://www.gao.gov/new.items/d10883t.pdf.

[32] See Ian Ayres and Steven D. Levitt, "Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack," *The Quarterly Journal of Economics* 113, no. 1 (1998), http://pricetheory.uchicago.edu/levitt/Papers/LevittAyres1998.pdf.

[33] Micah D. Lowenthal, testimony before the Senate Committee on Homeland Security and Government Affairs, June 30, 2010.

[34] In the interest of full disclosure, I wish to acknowledge having co-authored an analysis that posits several novel terrorist plots, including an attack that exploits the partisan political climate in the United States and another involving the manufacture of fake evidence of U.S. malfeasance to enrage the global Muslim community. See Dallas Boyd and James Scouras, "The Dark Matter of Terrorism," *Studies in Conflict & Terrorism* 33, no. 12 (December 2010). I further wish to acknowledge my indebtedness to my co-author in that endeavor, Dr. James Scouras, whose reflection on the wisdom of positing creative attack scenarios was the inspiration for this paper.

[35] Linda Rothstein, Catherine Auer, and Jonas Siegel, "Rethinking Doomsday," *Bulletin of the Atomic Scientists*, November/December 2004, http://www.mankindsmanycrossroads.com/Special-Interest/SI-doomsday-112504-1.htm.

[36] Jean Kumagai, ed., "Nine Cautionary Tales," *IEEE Spectrum*, September 2006, http://spectrum.ieee.org/computing/networks/nine-cautionary-tales/0.

[37] Thomas Homer-Dixon, "The Rise of Complex Terrorism," *Foreign Policy*, 128, January/February 2002. Available at: http://www.homerdixon.com/download/rise_of_complex_terrorism.pdf.

[38] See the following literature, respectively: Philip E. Ross, "Agro-Armageddon," in Jean Kumagai, ed., "Nine Cautionary Tales," *IEEE Spectrum*, September 2006, http://spectrum.ieee.org/computing/networks/nine-cautionary-tales/0; and Robert A. Baird, "Pyro-Terrorism—The Threat of Arson-Induced Forest Fires as a Future Terrorist Weapon of Mass Destruction," *Studies in Conflict & Terrorism* 29, no. 5 (June 2006).

[39] Bruce Schneier, "Announcing: Movie-Plot Threat Contest," *Schneier on Security* (blog), April 1, 2006, http://www.schneier.com/blog/archives/2006/04/announcing_movi.html.

[40] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton, 2004), 339.

[41] Dan Collins, "'99 Report Warned Of Suicide Hijacking," CBS News, May 17, 2002 http://www.cbsnews.com/stories/2002/05/17/attack/main509471.shtml.

[42] Rex A. Hudson, "The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and Why?" (Washington, DC: Federal Research Division, Library of Congress, September 1999), 7, http://www.loc.gov/rr/frd/pdf-files/Soc_Psych_of_Terrorism.pdf. Additionally, *The 9/11 Commission Report* noted that a group of Algerian terrorists hijacked an Air France flight in 1994 with the reported intention of detonating the aircraft over Paris or flying it into the Eiffel Tower. See *The 9/11 Commission Report,* 345. Finally, a 1995 novel by Tom Clancy featured a Boeing 747 being crashed into the Capitol Building during a joint session of Congress, killing most of the presidential line of succession. See Tom Clancy, *Debt of Honor* (The Berkeley Publishing Group: 1995), 975.

[43] Peter Huck, "Hollywood goes to war," *The Age*, September 16 2002, http://www.theage.com.au/articles/2002/09/14/1031608342634.html. See also Sharon Weinberger, "Hollywood's Secret Meet," *Wired*, March 16, 2007, http://www.wired.com/dangerroom/2007/03/foiled_by_foia_/. Other examples include the Defense Threat Reduction Agency's "Thwarting an Evil Genius" study, the Army's "Mad Scientist" seminar, and the Department of Homeland Security's Analytic Red Cell office. See, respectively, Brian A. Jackson and David R. Frelinger, "Emerging Threats and Security Planning: How Should We Decide What Hypothetical Threats to Worry About?" RAND Corporation Occasional Paper, 2009, http://www.rand.org/pubs/occasional_papers/OP256/; Noah Shachtman, "Army Assembles 'Mad Scientist' Conference. Seriously," *Wired*, January 9, 2009, http://www.wired.com/dangerroom/2009/01/armys-mad-scien/; and John Mintz, "Homeland Security Employs Imagination," *Washington Post*, June 18, 2004, http://www.washingtonpost.com/wp-dyn/articles/A50534-2004Jun17.html. For an unclassified summary of the Mad Scientist seminar, see "The Future Operational Environment: 2008 Mad Scientist Future Technology Seminar," United States Army Training and Doctrine Command, Portsmouth, Virginia, August 19-21, 2008, http://www.wired.com/images_blogs/dangerroom/files/2008_Mad_Scientist_Report_Final1-1.doc.

[44] Huck, "Hollywood goes to war."

[45] Marvin J. Cetron and Owen Davies, "55 Trends Now Shaping the Future of Terrorism," *The Proteus Trends Series* 1, no. 2 (February 2008), http://www.carlisle.army.mil/proteus/docs/55-terror.pdf. Cetron, preparer of the report "Terror 2000: The Future Face of Terrorism," asserts that his work "foretold the deliberate crash of an airplane into the Pentagon." See Marvin J. Cetron, "Terror 2000: The Future Face of Terrorism," conference report of the 4th Annual Defense Worldwide Combating Terrorism Conference, Office of the Assistant Secretary of Defense for SO/LIC, June 24, 1994.

[46] Marvin J. Cetron, "A Question of When," *Newsmax*, December 2007.

[47] James M. Acton, M. Brooke Rogers, and Peter D. Zimmerman, "Beyond the Dirty Bomb: Re-thinking Radiological Terror," *Survival* 49, no. 3 (Autumn 2007), http://www.iiss.org/publications/survival/survival-2007/2007-issue-3/.

[48] Ibid.

[49] Charles R. Gallaway, testimony before the House Homeland Security Subcommittee on Transportation and Infrastructure Protection, Washington, DC, July 15, 2009, http://homeland.house.gov/SiteDocuments/20090715140250-63489.pdf.

[50] Cetron, "A Question of When."

[51] Alan Cullison, "Inside Al-Qaeda's Hard Drive," *Atlantic Monthly*, September 2004, http://www.theatlantic.com/magazine/archive/2004/09/inside-al-qaeda-rsquo-s-hard-drive/3428/. Zawahiri may have been referring to the media deluge that followed then-Secretary of Defense William Cohen's 1997 appearance on the ABC's "This Week," in which he held aloft a five-pound bag of sugar and asserted that an equivalent quantity of anthrax could kill half the population of Washington, DC. One account of Cohen's performance described the press response thusly: "The media took off from there, with a frenzy of television and press stories about the horrors of possible anthrax, smallpox, or plague attacks." See Jeanne Guillemin, *Anthrax: The Investigation of a Deadly Outbreak* (University of California Press: 2001), 248. I am grateful to Joshua Pollack for identifying this incident as the possible inspiration of Zawahiri's statement.

[52] Colbert I. King, "A Monument to Defenselessness?" *Washington Post*, May 6, 2000.

[53] King listed the source of the scenario as "government security experts and private security consultants who have warned the executive branch and Congress that the Mall's monuments and memorials are highly vulnerable to terrorist attack and vandalism." See King, "A Monument to Defenselessness?" The attraction of the Washington Monument to terrorists was revisited as recently as December 2010; see Philip Kennicott, "Iconic obelisk presents a monumental security issue," *Washington Post*, November 8, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/07/AR2010110704572.html

[54] James Surowiecki, *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies, and Nations* (New York: Random House, 2004).

[55] Elliot Panek, "Terrorism and Contagious Media," August 8, 2007, http://wtpdg.blogspot.com/2007/08/terrorism-and-contagious-media.html.

[56] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html.

[57] Eric Lichtblau, "The Education of a 9/11 Reporter," *Slate*, March 26, 2008, http://www.slate.com/id/2187498/.

[58] Risen and Lichtblau, "Bush Lets U.S. Spy on Callers."

[59] David Stout, "Bush Says U.S. Spy Program Is Legal and Essential," *New York Times*, December 19, 2005, http://www.nytimes.com/2005/12/19/politics/19cnd-prexy.html. As a further indication of the story's controversy, author Gabriel Schoenfeld wrote a scathing article in *Commentary* magazine suggesting that the *New York Times* had violated the Espionage Act of 1917 by disclosing the domestic wiretapping program. See Gabriel Schoenfeld, "Has the New York Times Violated the Espionage Act?" *Commentary*, March 2006.

[60] http://cryptome.org/eyeball/index.html

[61] John Cook, "Secrets and Lies: The Man Behind the World's Most Dangerous Website," *Radar*, August 13, 2007, http://cryptome.org/radar-smear.htm.

[62] Ibid.

[63] Spencer S. Hsu and Carrie Johnson, "TSA accidentally reveals airport security secrets," *Washington Post*, December 9, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/12/08/AR2009120803206.html. The original discovery was made by blogger Seth Miller, who posted the manual on his web site, WanderingAramean.com, and forwarded it to Cryptome.org for broader dissemination. See Jaikumar Vijayan, "Analysis: TSA Document Release Show Pitfalls of Electronic Redaction," *Computerworld*, December 11, 2009.

[64] Alison Grant, "Sensitive security guidelines revealed online—again," *Plain Dealer*, January 5, 2010, http://www.cleveland.com/business/index.ssf/2010/01/sensitive_tsa_security_guideli.html.

[65] *Report of the National Commission for the Review of the National Reconnaissance Office: The NRO at the Crossroads*, November 1, 2000, http://www.fas.org/irp/nro/commission/nro.pdf. Illustrating the danger of amateurs' tracking of classified satellites is a 2006 article in *Wired* magazine, which recounts an ominous conversation between Canadian satellite tracker Ted Molczan and an unidentified caller during the Persian Gulf War. Molczan, an accomplished observer of U.S. spy satellites, received a phone call on the first day of the war from a man speaking heavily accented English. The caller requested information on the orbits of American KH-11 "Key Hole" satellites, which were then being used to conduct surveillance over Iraq and Kuwait. According to the article, the incident forced Molczan to "think about what would happen if the information collected by those 'in the [satellite tracking] hobby' ever ended up in the wrong hands." Nevertheless, the experience "hasn't changed the way he works." See Patrick Radden Keefe, "I Spy," *Wired*, Issue 14.02, February 2006, http://www.wired.com/wired/archive/14.02/spy.html.

[66] William J. Broad, "Surveillance Suspected as Spacecraft's Main Role," *New York Times*, May 22, 2010, http://www.nytimes.com/2010/05/23/science/space/23secret.html?_r=1&hp. See also Leonard David, "Secret X-37B Space Plane Spotted by Amateur Skywatchers," Space.com, May 22, 2010, http://www.space.com/news/secret-x-37-b-space-plane-spotted-by-amateur-astronomers-100522.html.

[67] Rosemary Chalk, "Security and Scientific Communication," *Bulletin of the Atomic Scientists*, August/September 1983. The same year, Adm. Bobby R. Inman, then-Deputy Director of the CIA, observed in a controversial speech that there were "fields where publication of certain technical information could affect the national security in a harmful way." Inman suggested that a balance between national security and scientific research might be found by agreeing to include the "question of potential harm to the nation" in the peer review process. At the time, a similar agreement was already in place that allowed the National Security Agency (NSA) to review cryptography-related manuscripts and recommend modifications prior to publication. See Bobby R. Inman, "Classifying Science: A Government Proposal..." *Aviation Week & Space Technology*, February 8, 1982; see also Dale R. Corson, Chair, *Scientific Communication and National Security* (Washington, DC: National Academies Press, 1982), 3.

[68] Dale R. Corson, Chair, Panel on Scientific Communication and National Security Committee on Science, Engineering, and Public Policy, National Academy of Sciences, *Scientific Communication and National Security* (Washington, DC: National Academies Press; September 30, 1982), http://www.nap.edu/catalog.php?record_id=253.

[69] Nicholas Wade, "Panel of Scientists Supports Review of Biomedical Research That Terrorists Could Use," *New York Times*, October 9, 2003. See also Herbert N. Foerstel, *Secret Science: Federal Control of American Science and Technology* (Westport: Praeger, 1993).

[70] Corson, *Scientific Communication and National Security*, 48. See also National Security Decision Directive (NSDD)-189, "National Policy on the Transfer of Scientific, Technical and Engineering Information," September 21, 1985, http://www.fas.org/irp/offdocs/nsdd/nsdd-189.htm. NSDD-189 stated, "It is the policy of [the Reagan] Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted."

[71] Ronald J. Jackson et al., "Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox," *Journal of Virology* 75, no. 3 (2001), www.ncbi.nlm.nih.gov/pmc/articles/PMC114026/pdf/jv001205.pdf.

[72] Michael J. Selgelid and Lorna Weir, "The Mousepox Experience," *EMBO reports* 11 (2010): 18-24, http://www.nature.com/embor/journal/v11/n1/full/embor2009270.html.

[73] Jon Cohen, "Designer Bugs," *Atlantic Monthly*, July/August 2002, http://www.theatlantic.com/past/docs/issues/2002/07/cohen-j.htm.

[74] Wade, "Panel of Scientists Supports Review of Biomedical Research." See also Selgelid and Weir, "The Mousepox Experience."

[75] Wade, "Panel of Scientists Supports Review of Biomedical Research." A later, similarly controversial scholarly publication concerned the reconstructed genome of the 1918 influenza virus, commonly referred to as the "Spanish Flu," which killed between 50-100 million people worldwide. See T.M. Tumpey, C.F. Basler, P.V. Aguilar et al., "Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus," *Science* 310 (2005). See also Phillip A. Sharp, "1918 Flu and Responsible Science," *Science* 310 (2005). Yet another controversial piece of research involved the synthesis of the poliovirus. See Jeronimo Cello, Aniko V. Paul, and Eckard Wimmer, "Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template," *Science* 297, no. 5583 (August 9, 2002), http://www.sciencemag.org/cgi/content/abstract/1072266.

[76] Ronald Atlas, "Conducting Research During the War on Terrorism: Balancing Openness and National Security." Testimony before the House Committee on Science, October 10, 2002, http://www.asm.org/Policy/index.asp?bid=5703. As cited in Elisa D. Harris and John D. Steinbruner, "Scientific Openness and National Security After 9-11," *CBW Conventions Bulletin*, No. 67 (March 2005).

[77] Scott Shane, "Terror threat casts chill over world of bio-research; Arrest of Texas professor highlights emergence of security as a major issue," *The Baltimore Sun*, January 26, 2003.

[78] "Statement on Scientific Publication and Security," *Science* 299, no. 5610 (February 21, 2003), http://www.sciencemag.org/cgi/content/short/299/5610/1149.

[79] National Research Council Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, *Biotechnology Research in an Age of Terrorism* (Washington, DC: The National Academies Press, 2004), 101, http://www.nap.edu/catalog.php?record_id=10827.

[80] Ibid., 8. The panel also recommended the establishment of a National Science Advisory Board for Biodefense to provide guidance on policies to prevent the misuse of research in the life sciences (see pages 8-9). For a later NAS report that grapples with the dual-use dilemma, see National Research Council Committee on a New Government-University Partnership for Science and Security, *Science and Security in a Post 9/11 World: A Report Based on Regional Discussions Between the Science and Security Communities* (Washington, DC: The National Academies Press, 2007), http://books.nap.edu/catalog.php?record_id=12013. See also Dana A. Shea, "Balancing Scientific Publication and National Security Concerns: Issues for Congress," Congressional Research Service report, February 2, 2006, www.fas.org/sgp/crs/secrecy/RL31695.pdf.

[81] *Biotechnology Research in an Age of Terrorism*, 26.

[82] Ibid., 27.

[83] Ibid.

[84] Selgelid and Weir, "The Mousepox Experience."

[85] Scott Shane, "Paper Describes Potential Poisoning of Milk," *New York Times*, June 29, 2005, http://www.nytimes.com/2005/06/29/politics/29milk.html.

[86] Lawrence M. Wein and Yifan Liu, "Analyzing a Bioterror Attack on the Food Supply: The Case of Botulinum Toxin in Milk," *Proceedings of the National Academy of Sciences of the United States of America* 102, no. 28 (July 12, 2005), http://www.jstor.org/stable/3376090.

[87] Lawrence M. Wein, "Got Toxic Milk?" *New York Times*, May 30, 2005, http://www.nytimes.com/2005/05/30/opinion/30wein.html

[88] Scott Shane, "Paper Describes Potential Poisoning of Milk," *New York Times*, June 29, 2005, http://www.nytimes.com/2005/06/29/politics/29milk.html.

[89] Bruce Alberts, "Modeling attacks on the food supply," *Proceedings of the National Academy of Sciences* 102, no. 28 (July 12, 2005), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1175018/pdf/pnas-0504944102.pdf.

[90] Dan Stober, "No Experience Necessary," *Bulletin of the Atomic Scientists*, March/April 2003. For a declassified summary of the original report, see W.J. Frank, "Summary Report of the Nth Country Experiment," (Livermore, CA: Lawrence Radiation Laboratory, University of California, March 1967), http://www.gwu.edu/~nsarchiv/news/20030701/nth-country.pdf

[91] Howard Morland, "The H-bomb Secret: To Know How is to Ask Why," *Progressive* 43 (November 1979): 14-23.

[92] United States of America v. *The Progressive*, Inc., Erwin Knoll, Samuel Day, Jr. and Howard Morland, 467 F. Supp. 990 (W.D. Wis, 1979). For additional information on the *Progressive* case, see Alexander De Volpi et al., *Born Secret: The H-bomb, the Progressive Case and National Security* (New York: Pergamon Press, 1981); Samuel Day, Jr., "The Other Nuclear Weapons Club: How the H-bomb Amateurs Did their Thing," *Progressive* 43 (November 1979): 33-37; and Erwin Knoll, "Wrestling with Leviathan: The Progressive Knew it Would Win," *Progressive* 43 (November 1979): 24.

[93] Edward Herman, "A Post-September 11th Balancing Act: Public Access to U.S. Government Information Versus Protection of Sensitive Data," *Journal of Government Information* 30, no. 42 (2004).

[94] Laura Blumenfeld, "Dissertation Could Be Security Threat," *Washington Post*, July 8, 2003, http://www.washingtonpost.com/ac2/wp-dyn/A23689-2003Jul7?language=printer.

[95] Ibid.

[96] *Freakonomics* author Steven D. Levitt describes a scenario for achieving a similar effect on a national scale: "The basic idea is to arm 20 terrorists with rifles and cars, and arrange to have them begin shooting randomly at pre-set times all across the country… Have them move around a lot. No one will know when and where the next attack will be. The chaos would be unbelievable…." See Steven D. Levitt, "If You Were a Terrorist, How Would You Attack?" Freakonomics blog, *New York Times*, August 8, 2007, http://freakonomics.blogs.nytimes.com/2007/08/08/if-you-were-a-terrorist-how-would-you-attack/

[97] Carrie Johnson and Spencer S. Hsu, "Terrorism Suspect Planned Peroxide Bombs, Officials Say," *Washington Post*, September 25, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/09/24/AR2009092400332.html

[98] David M. Rabban, *Free Speech in Its Forgotten Years* (New York: Cambridge University Press, 1997).

[99] Pluchinsky, "They Heard it all Here."

[100] In another context, this phenomenon is sometimes referred to as the "Streisand effect" after entertainer Barbra Streisand's effort to embargo aerial photographs of her beachfront Malibu mansion. This attempt had the unintended consequence of ensuring that the photographs reached a far greater audience than would have otherwise been the case. I am indebted to Joshua Pollack for bringing this term to my attention.

[101] Hugh E. DeWitt, "Has U.S. Government Disclosed the Secret of the H-Bomb," *Bulletin of the Atomic Scientists*, April 1979.

[102] Sean D. Naylor, "Censored Book Masks Sensitive Operations," *Army Times*, October 4, 2010, http://www.armytimes.com/news/2010/10/army-book-100410w/.

[103] Scott Shane, "Secrets in Plain Sight in Censored Book's Reprint," *New York Times*, September 17, 2010, http://www.nytimes.com/2010/09/18/us/18book.html?_r=1. Among the redacted items was the observation that "Guys on phones were always great sources of [intelligence]…." See Steven Aftergood, "Behind the Censorship of Operation Dark Heart," *Secrecy News* 2010, no. 78 (September 29, 2010), http://www.fas.org/sgp/news/secrecy/2010/09/092910.html. For a side-by-side comparison of redacted vs. original content in the censored version of Operation Dark Heart, see: http://www.fas.org/sgp/news/2010/09/dark-contrast.pdf.

[104] Sean D. Naylor, "Censored Book Masks Sensitive Operations."

[105] Donald Kennedy, "Better Never Than Late," *Science* 310, no. 5746 (October 14, 2005), http://www.sciencemag.org/cgi/content/summary/310/5746/195

[106] Jaffe and DeYoung, "Leaked files lay bare war in Afghanistan," and Miller and Finn, "Secret Iraq war files offer grim new details."

[107] "Internet Content Advisory: Considering The Unintended Audience," Advisory 02-001, National Infrastructure Protection Center, January 17, 2002, http://www.iwar.org.uk/infocon/advisories/2002/02-001.htm. An earlier admonition was issued in the National Infrastructure Protection Center's (NIPC) publication *Highlights*, which advised "Risk management should be considered when reviewing materials for web dissemination, balancing the sharing of information against potential security risks." See "Terrorists and the Internet: Publicly Available Data should be Carefully Reviewed," *Highlights*, National Infrastructure Protection Center, December 7, 2001, http://www.iwar.org.uk/infocon/nipc-highlights/2001/highlight-01-11.pdf. The NIPIC, originally situated within the FBI, was transferred to the Department of Homeland Security when the agency was established in March 2003.

[108] Peter J. Westwick, "In the Beginning: The Origin of Nuclear Secrecy," *Bulletin of the Atomic Scientists*, 56, no 6 (November/December 2000): 43-49.

[109] Anthony Lewis, "More Than Fit to Print," *New York Review of Books*, April 7, 2005. http://www.nybooks.com/articles/archives/2005/apr/07/more-than-fit-to-print/. As cited in John Prados and Margaret Pratt Porter, eds., *Inside the Pentagon Papers* (University Press of Kansas: 2004), 10.

[110] Acton et al., "Beyond the Dirty Bomb."

[111] Laurie Garrett, *Betrayal of Trust: The Collapse of Global Public Health* (New York: Hyperion, 2000), 540-541.

[112] Corson, *Scientific Communication and National Security*, 5-6.

[113] Selgelid and Weir, "The Mousepox Experience." It should be noted that this statement, made by Dr. Ian Ramshaw, appears to contradict another remark he made in the same interview (cited earlier in this article) that "the original [mousepox] work should never have started in the first place." If the research was sufficiently dangerous to argue against its being conducted at all, it is not clear why the findings of the research, however "interesting," should be made public. I can find no explanation for the logical dissonance between these two comments.

[114] Michael S. Sweeney, *Secrets of Victory: The Office of Censorship and the American Press and Radio in World War II* (Chapel Hill: The University of North Carolina Press, 2001).

[115] Bob Woodward, *The War Within: A Secret White House History (2006–2008)* (New York: Simon & Schuster, 2008).

[116] Lou Michel and Dan Herbeck, *American Terrorist: Timothy McVeigh and the Oklahoma City Bombing* (Regan Books, 2001).

[117] If access to a workable design is a crucial ingredient in a state nuclear weapon program, it stands to reason that the same may true for the bombs of less sophisticated terrorists. See Li Bin, "An alternative view to North Korea's bomb acquisition," *Bulletin of the Atomic Scientists* 66, no. 3 (May/June 2010).

[118] "Terror Risk as Deadly Nerve Gas Secrets Are Revealed," *Sunday Times*, January 5, 1975.

[119] For a detailed history of the Sunday Times story and the subsequent response of the British Government, see Brian Balmer, "A Secret Formula, a Rogue Patent and Public Knowledge about Nerve Gas: Secrecy as a Spatial-Epistemic Tool," *Social Studies of Science* 36 (2006): 691-722.

[120] Ibid.

[121] Ibid.

[122] Geoffrey E. Forden, "How the World's Most Underdeveloped Nations Get the World's Most Dangerous Weapons," *Technology and Culture* 48, no. 1 (January 2007), http://web.mit.edu/stgs/pdfs/TandC_essay_on_WMD.pdf.

[123] Brian Knowlton, "Leaked Cable Lists Sensitive Sites," *New York Times*, December 6, 2010, http://www.nytimes.com/2010/12/07/world/07sites.html?_r=1.